Testimony of

Mary R. Grealy
President
Healthcare Leadership Council

Before the

American Health Information Community
Confidentiality, Privacy, and Security Working Group

June 22, 2007

I want to thank you on behalf of the members of the Healthcare Leadership Council (HLC) for the opportunity to testify before the American Health Information Community's Working Group on Confidentiality, Privacy and Security on the Health Insurance Portability and Accountability Act of 1996's (HIPAA) privacy rule and how it will protect patient privacy in an environment of electronic clinical health information exchange.

HLC is a not-for-profit membership organization comprised of chief executives of the nation's leading health care companies and organizations, with membership that includes hospitals, health plans, pharmaceutical companies, medical device manufacturers, biotech firms, health product distributors, pharmacies and academic medical centers. Fostering innovation and constantly improving the affordability and quality of American health care are all goals uniting HLC.

While I know that many of you on the panel are familiar with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule, I think it would be useful to revisit the deliberations about privacy during development of both the House and Senate legislation -- drafted in response to HIPAA's enactment -- and the Privacy Rule itself. Those intensive, comprehensive deliberations over a five-year period carefully weighed the competing interests in our extraordinarily complicated health care system. They included both a Democrat and Republican Administration and thus experts from both political parties. The result of these deliberations we believe to be an effective privacy rule.

For more than ten years, HLC has chaired the "Confidentiality Coalition,"[1] a broad-based group of organizations that support nationally uniform privacy standards. During Congressional enactment of the (HIPAA) statute and regulatory development of the HIPAA Privacy Rule, the Confidentiality Coalition played a leadership role, working with members of Congress and the administration to advocate for a workable privacy

[1] The Confidentiality Coalition includes over 100 physician specialty and subspecialty groups, nurses, pharmacists, employers, hospitals, nursing homes, biotechnology researchers, health plans, pharmaceutical benefit management and pharmaceutical companies.

rule. Today, the Coalition continues to help educate members of Congress about the protections afforded in the Privacy Rule to avoid conflicting or duplicate legislation.

We sought a rule that would strike the appropriate balance between protecting the sanctity of a patient's medical information privacy while, at the same time, ensuring that necessary information is available for providing quality health care and conducting vital medical research. We advocated for a rule with effective confidentiality safeguards that would not burden providers and patients with unnecessary paperwork or delays in treatment. We believe that the Privacy Rule to a great extent achieved this balance and has increased consumers' confidence in the privacy of their medical records.

Covered entities take compliance with the Privacy Rule very seriously. Health care providers, payers and other covered entities as well as their business associates have implemented comprehensive training and compliance plans to adhere to the Privacy Rule. Under the Privacy Rule, disclosing identifiable health information for purposes other than carefully defined, appropriate health-care activities is prohibited unless the patient grants specific, prior written authorization. The statute carries strong civil and criminal penalties for non-compliance.

In addition, since April of 2005, covered entities must also be in compliance with the HIPAA Security Rule. The Security Rule applies to electronic protected health information that a covered entity creates, receives, maintains, or transmits. The rule requires covered entities to protect against threats or hazards to the security or integrity of information, as well as uses and disclosures not allowed by the privacy rule.

Ongoing dialogue about health information technology and standards for the electronic transaction of health care has raised questions about the privacy and security of electronic health information in an electronic context. I think it is of the utmost importance to note that it was concern about the impact on patient privacy of the health system widely adopting *electronic* transactions that spurred the HIPAA privacy rule. Thus, during the rulemaking process for the Health Insurance Portability and

Accountability Act (HIPAA) Privacy and Security rules, many of these same questions were discussed, and the result is that the HIPAA Privacy and Security rules include ample provisions governing the confidentiality of patient medical information, electronic or otherwise.

We are concerned that some policymakers may not be aware of the purpose and scope of the HIPAA privacy and security rules and will advocate for additional, burdensome privacy regulations for electronic health records. The current HIPAA regulations are very restrictive and health care organizations like our members have taken a very conservative compliance approach in their business practices. I think many consumers will attest to this fact if they have attempted to get health care claims or medical information for themselves or another person, such as a parent, without a prior approved authorization. Some have expressed concerns about “hyper-compliance” with the Privacy Rule.

We understand that many believe that the HIPAA privacy rule must be revised in light of electronic transfer of data and web-based access to personal health records, so that patients may trust that the system will keep their data private. We share the belief that patients' confidence in health information technology systems is of the utmost importance in order for them to be successful. We believe that it is vitally important that patients understand the protections contained in the HIPAA rule, so they can be confident that their records are and will be protected. We also need to do a better job informing patients and consumers how appropriate access to their health information will improve the quality of their health care and the care of future generations.

I. National Uniform Standard for Privacy

One area of concern regarding the privacy rule is the rule's lack of a national uniform standard for privacy. Though we strongly believe that the HIPAA privacy rule provides a sound basis for protecting health information, progress toward electronic data exchange is significantly impeded by the lack of a uniform federal privacy standard.

As an underpinning for our discussion today, we've attached a map developed by the Indiana Network for Patient Care (Fig.1). Each dot represents a patient seen at an Indianapolis hospital during a six-month period. While the dots are stacked very deep around Indianapolis as you would expect, patients served by the Indiana hospitals during this period were also located in 48 of the 50 states. Today's health care providers, meeting the needs of a mobile society, serve patients from multiple and far-flung jurisdictions. Looking at this map it is easy to see why local and regional agreements will not be adequate to address the myriad regulations with which providers and others will need to comply to achieve interoperability and why national standards, not just for interoperability, but also for privacy and data security, are necessary.

Although HIPAA establishes a federal privacy standard, it permits significant state variations that we believe will create serious impediments to interoperable sharing or sending of health information, particularly across state lines. This is true not only with respect to the technical standards employed through information technology, but also with respect to the privacy standards that govern information disclosures.

In addition, since the Privacy Rule does not supersede state privacy laws, providers, clearinghouses and health plans are required to comply with the federal law as well as any state privacy restrictions that are contrary and more stringent. In the context of HIPAA implementation this has been extremely difficult and in the context of broad and widespread health information exchange it may be nearly impossible, as the RTI International study undertaken by AHRQ is discovering. In summary, state stakeholders are identifying a general misunderstanding regarding the many potential intersections of present state laws and HIPAA, finding that state laws do not currently address or apply sensibly to the proposed electronic exchange of health information.[2]

[2] "Health Information Security and Privacy Collaboration Hosts National Meeting to Discuss Stakeholder Concerns," RTI International, April 1, 2007.

State health privacy protections vary widely and are found in thousands of statutes, regulations, common law principles, and advisories. Health information privacy protections can be found in a state's health code as well as its laws and regulations governing criminal procedure, social welfare, domestic relations, evidence, public health, revenue and taxation, human resources, consumer affairs, probate and many others. While Indiana uses HIPAA as its state privacy law, virtually no other state requirement is identical to the federal rule. Within a given state, privacy laws may actually conflict, adding to confusion among those who hold identifiable health information and those who seek to set up data exchanges.

HHS will not provide a comprehensive preemption analysis of these state privacy protections. Moreover, single-state and private-sector efforts have been extremely costly, do not utilize consistent standards, and are difficult to manage against the constantly changing 50-state environment. HLC and the Confidentiality Coalition attempted to address this problem directly by commissioning a multi-jurisdiction study of this issue and quickly assessed costs of more than $1 million with $100,000 for annual updates. Unfortunately many organizations, particularly smaller provider groups, do not have such resources and must navigate the sea of privacy regulations and laws on their own.

The federally funded RTI study is looking at only 33 states, not all 50, and focusing on working with state organizations to determine what laws exist in each state and what organizations are doing to streamline state statutes and regulations to make them consistent within each state, so that data may be exchanged more easily within a given state. But looking at the Indiana chart referenced above, it is unfortunate that the RTI study did not do a thorough analysis of how state laws are impeding movement of information across state lines.

From the discussions of RTI study participants (i.e., those of the March 5-6 conference convening the state officials and project managers involved in the RTI study) it appears that even within each state many organizations are unable to discern the appropriate

statutes and regulations, and instead their legal departments seem simply to establish a privacy policy with which they are comfortable, refusing to exchange data with any but trusted partners. While this is completely understandable in the context of the wide range of state laws and regulations, it bodes poorly for electronic data exchange, especially across state lines, as the Indiana map demonstrates.

Interestingly, the exception may be Indiana, where, because HIPAA essentially serves as the state's health privacy law, the state is proceeding with a state-wide health information exchange.

HLC is not alone in calling for nationally uniform privacy standards. The 11-member Commission on Systemic Interoperability, authorized by the Medicare Prescription Drug, Modernization, and Improvement Act to develop recommendations on HIT implementation and adoption, recommended that Congress authorize the Secretary of HHS to develop a uniform federal health information privacy standard for the nation, based on HIPAA and preempting state privacy laws, in order to enable data exchange interoperability throughout the country.

While we believe strongly in the need for a national privacy standard, HLC believes just as strongly that any regional or national system designed to facilitate the sharing of electronic health information must protect the confidentiality of patient information. It is not our intent in calling for one national privacy standard to weaken privacy protections for individuals, but rather to facilitate nation- and system-wide electronic interchange of data.

II. Patient Consent and Control

At the center of the dialogue about electronic health records and information is the question of patient consent and control. After lengthy debate, the final HIPAA Privacy Rule as modified allows covered entities to use patients' medical information without prior authorization for medical treatment, claims payment or health care operations or

as otherwise permitted or required[3]. For other uses, providers must obtain a written authorization from each patient.

Requiring providers and payers to obtain prior consent to use individually identifiable health information for treatment, payment and health care operations was rejected because of concerns that a prior authorization requirement would seriously delay and disrupt the care of patients, particularly the most vulnerable patients. For example, elderly patients would not be able to send a family designee to a pharmacy to pick up a prescription without first going to the pharmacy to sign consent forms; pharmacies would not be able to fill prescriptions phoned in by physicians until the patient arrived to give consent; and emergency medical personnel would be forced to get consent forms signed before treating patients – even when contrary to best medical practice. These concerns were not simply theoretical; Maine enacted a law requiring prior consent to use patient-identifiable information for health care purposes. The law was suspended just 12 days after taking effect because of the chaos that ensued in hospitals and pharmacies.

The much-touted benefits of health IT, most importantly improvement of quality of care through better patient outcomes, will not be realized if information exchange is constrained by various authorization or consent requirements. Far worse, adding such requirements in the context of health information exchange will slow and impede providers' current ability to deliver health care services. Thus, in general, we believe that changing the rule's provisions regarding consent and control would be unnecessary and harmful.

In recent years, the advent of personal health records (PHRs) has triggered another set of discussions about patient control of their health information. We agree that with respect to PHRs, individuals will want to control distribution. We are seriously

[3] Under the Privacy Rule a covered entity is permitted to use and disclose protected health information without authorization for the following purposes or situations: 1) to the individual; 2) for treatment, payment and health care operations; 3) for uses and disclosures with an opportunity to agree or object; 4) for uses and disclosures that occur incident to an otherwise permitted use or disclosure; 5) for public interest and benefit activities; and 6) of a limited data set for purposes of research, public health or health care operations.

concerned about the prospects of allowing consumers to control which health care providers may see their medical records and the portions of the records that may be shared, even after the patient has entered the health care system for treatment. We caution against allowing or expecting a fully patient-controlled PHR to become a *de facto* electronic health record for use in clinical settings, as physicians will never trust that they have accurate and complete information if they know that patients can withhold pieces of the record.

We would suggest that while PHRs may be controlled by individuals, once their information reaches an EHR, it should be used and disclosed as under HIPAA, allowing for information to move within the health care system, including via electronic data exchange, as it may under HIPAA, which will facilitate optimal patient care and data available to improve health care quality.

If patients may direct where information may flow within the health care system, it will upset HIPAA's careful calibration, designed to facilitate providers having all the necessary facts for proper diagnosis and treatment. Enabling patients to direct what information may be shared electronically is the same as saying patients may direct what information is withheld from their physicians, researchers and accreditors. Critical data could be omitted from aggregated data made available to researchers hoping to improve health care quality and patient outcomes. In addition, providers are very concerned about the liability that might result from their reliance on incomplete information.

We often hear the argument that physicians already are relying on incomplete information and that at least a partial record would be an improvement. We would respond that given the resources that will be required to implement health IT, it would be irresponsible to build into a new, more expensive medical records system the same drawbacks that are inherent in our current, largely paper-based system. If we want to retain the inefficiency and lack of data of the current system, the nation does not need to spend billions of dollars on health information technology.

We agree that use of a national, regional, or even local health care information exchange will require patient and consumer confidence. It will be crucial to educate consumers and patients about the privacy protections and penalties enacted under HIPAA and the Security Rule. However, providers too must have confidence in the integrity of the data provided through health information exchange in order to assure utilization of such a system. In evaluating proposals to require consent or varying degrees of patient control, we urge the Working Group to carefully consider the ramifications for health care delivery and public health that such steps would impose.

Addressing this issue appropriately will be essential to achieving the interoperability necessary to improve the quality and cost effectiveness of the health care system – while still assuring patients' confidence that their information will be kept private.

HLC has some additional comments about the HIPAA privacy rule, but given the questions you have asked us to address in this meeting, we have reserved them in an addendum to the testimony and will move on to more directly address some of your questions.

III. HIPAA Expansion in Health Information Exchange

You have asked us to address the topic of whether HIPAA is sufficient within the context of health information exchange. As participants throughout the process of developing first HIPAA and then the privacy rule, we believe that policymakers worked diligently to foresee how information would move in the coming years. Indeed, the rule works very well for health information exchange within HIPAA covered entities and activities.

In addition, other entities beyond HIPAA covered entities comply with the privacy rule's requirements. "Business Associates" of covered entities, those that perform certain functions or activities on behalf of a covered entity, or provide services to a covered entity that involve the use or disclosure of individually identifiable health information, are

contractually bound to the rule's standards and thus are contractually prohibited from making any use or disclosure of protected health information that would violate the Privacy Rule.

What the rule did not contemplate was the broad movement to web-based technology, instead of electronic medical records housed within providers' offices or at hospitals. In an internet-based world, many organizations may have access to protected health information, some without the patient's knowledge. Those that are not already complying with HIPAA, either as a covered entity or business associate, should be included as HIPAA-covered entities. For example, health information exchanges could be regulated as HIPAA-covered entities if they cannot be determined to qualify as health care clearinghouses.

Regulation of personal health records (PHRs) is somewhat less clear. Under current scenarios, individuals give PHR companies permission to hold their data, which the company maintains for them in a record, and which the company will send to clinicians and health care providers upon the authorization of the patient. To date, the companies providing PHRs include health plans, stand-alone organizations, and divisions of larger, diversified companies who may not be health care companies. To the extent that these records are held by health plans, they appear to be captured under HIPAA. To the extent that they are not held by health plans, they are essentially unregulated, other than through the contractual agreements that the companies have with the individuals whose records they hold or applicable state privacy laws.

It is in the companies' best interests to keep identifiable information confidential, and to date, they all profess to adhere to extremely strict privacy standards. Assuming that the value of the record is in its storage and transmission, we can expect companies to adhere to their strict privacy protections. Should the value of the records for other purposes exceed their value for maintenance and distribution, then the records are somewhat less likely to be kept confidential.

The HLC would support reasonable efforts to ensure that personal health records held by organizations that are not HIPAA-covered entities meet HIPAA privacy and security rule requirements. The challenge, however, is how to structure such a requirement, so as not to stifle innovation that engages individuals in better managing their health.

One possibility would be to deem health information exchanges as health care clearinghouses for the sake of simplicity.

The ramifications of extending HIPAA coverage to other entities must be carefully considered, but we strongly believe that to the extent that additional entities are brought into federal privacy protections, it is critically important not to upset the carefully calibrated balance HIPAA has struck with respect to access to information and confidentiality.

Conclusion

In conclusion, I want to thank you again for the opportunity to testify before the Working Group. HLC strongly supports the broader implementation of HIT – HIT offers unparalleled potential for improvement in health care quality. However, patients' confidence in the confidentiality and security of the HIT infrastructure that is built is essential in order for the resources spent on HIT acquisition and development to be meaningful.

We would urge the Working Group's careful consideration of the ramifications of changes to the federal regulations governing patient confidentiality. Such changes, if any, should be measured and deliberate in order to continue the successful track record set by the HIPAA privacy rule.

Health care providers, plans and clearinghouses have spent significant resources to comply with the HIPAA privacy rule. Before recommending changes to the rule, we should be absolutely certain that such changes are indeed necessary in order to justify

the diversion of scarce resources from patient care to additional administrative compliance.

Multi-state electronic exchange of data is already occurring, as health plans, pharmacy benefit managers, pharmacists use their interconnected electronic systems to pay claims, fill and pay for prescriptions, operate disease management programs, and alert patients and clinicians to important information. While patients and clinicians are as yet unused to accessing medical files electronically, the HIPAA privacy and security protections for identifiable information have worked very well to keep patient-identifiable information confidential. There is no reason to believe that these same protections, which were drafted with the electronic transmission, health care treatment and patient information in mind, will not work equally well for expanded exchange of clinical information.

We look forward to working with the Working Group further. Any questions about my testimony or these issues can be addressed to me at the Healthcare Leadership Council (telephone 202-452-8700, e-mail mgrealy@hlc.org).

Addendum: Other concerns about HIPAA's current requirements in the context of HIT

IV. Minimum Necessary

HLC believes that the Privacy Rule's minimum necessary standard – which already poses significant burdens for covered entities – may be unworkable in the context of disclosures made through health information exchange from health care providers. The Privacy Rule provides that covered entities must make "reasonable efforts" when using, disclosing or requesting protected health information, to limit the information to the "minimum necessary" amount needed to accomplish the intended purpose of the use, disclosure or request. In addition, the regulation provides that covered entities may not use, disclose or request an entire medical record unless the entire record is "specifically justified" as the amount of information reasonably necessary. Disclosures to, or requests by, a provider for treatment purposes are exempt from the standard as are uses or disclosures made pursuant to a written patient authorization. A covered entity may rely on a requested disclosure of protected health information from another covered entity as being the minimum necessary amount.

This standard puts covered entities receiving requests to disclose information in the position of determining whether the requested information is the "minimum necessary" amount, when only the entity making a request for information has an informed basis for determining whether the information is the minimum necessary for its purposes. The legal uncertainty and risk created by this standard already has led to some "defensive" information practices that restrict the appropriate flow of information within the health care system. For example, some providers, citing the need to comply with the HIPAA Privacy Rule, have limited access by health plans to protected health information needed to perform quality assessment and improvement programs, utilization review, case management, disease management, and other functions related to maintaining the affordability of health coverage and improve outcomes.

Especially in an era of increasing interest in comparing the effectiveness of treatments, it is critically important that information be available to those who may legally access it for legitimate reasons, such as determining the relative effectiveness of one treatment versus another, and that patient control of information or citations of the minimum necessary requirements not be used to subvert attempts to determine optimal and efficient treatments for patients.

For participants in a national or regional health information network, making minimum necessary determinations – or even determining if a requesting party or provider is a HIPAA covered entity – is likely to be extremely challenging. The uncertainty and resultant liability exposure associated with the minimum necessary standard is likely to serve as a barrier to participation in health information exchange. Interoperability and information exchange across healthcare settings cannot be fully met if a physician is required to adhere to a nebulous minimum necessary standard. The application of the minimum necessary standard to this effort may in fact increase medical error rates by limiting the flow of medical information in the health care system in a manner that is inconsistent with the provision of quality medical care. Consideration should be given to eliminating the standard, or creating a safe harbor for when personal health information is exchanged through a national health information network or regional health information exchange.

V. Research

We are also concerned that current-law restrictions in the area of research will prevent health information exchange from achieving its ultimate objective as a tool to improve quality of care.

Research uses and disclosures are an essential part of the national HIT infrastructure envisioned in many scenarios, especially as it pertains to improvement of patient care. The data collected in this effort will be crucial to achieving key objectives of this initiative,

particularly the goal of improving population health by accelerating the movement of the fruits of research into delivery systems in a meaningful way.

The HIPAA Privacy Rule also recognizes the importance of research to improving the quality of health care and took steps to ensure that researchers would have continuing access to health information. Under the Privacy Rule, numerous entities, including non-covered entities, receive and analyze de-identified data or limited data sets to assist health care providers, health plans, government, the health care management communities and manufacturers conduct market, utilization and outcomes research, implement best practices, and apply and benefit from economic analyses. Data researchers have helped implement prescription drug recall programs, performance of pharmaceutical market studies, and assessment of drug utilization patterns. In these areas and many others the HIPAA framework took care to protect patient privacy while permitting data use for research where appropriate.

We are concerned, however, that in some instances the HIPAA Privacy Rule failed to achieve the proper balance and is inappropriately restricting access to health information for researchers. In particular, requiring expiration dates or events on all research authorizations and prohibiting individuals from granting authorization to use their health data in unspecified future studies is limiting the on-going use of research data in ways that are detrimental to the health care system. Under the Common Rule that has governed human subjects research for decades, it is generally permissible to obtain informed consent from a participant to use data for future research on data or biologic materials stored in databases or tissue banks. The Privacy Rule does not permit authorization for virtually any unspecified future uses. The Secretary's Advisory Committee on Human Research Protections (SACHRP) has recommended that the HIPAA Privacy Rule permit future uses that are allowed under the Common Rule. We agree that the Privacy Rule needs to be modified in this area to be consistent and note that these restrictions, if not addressed, will have a significant impact on the ability of stakeholders to achieve critical goals of HIT.

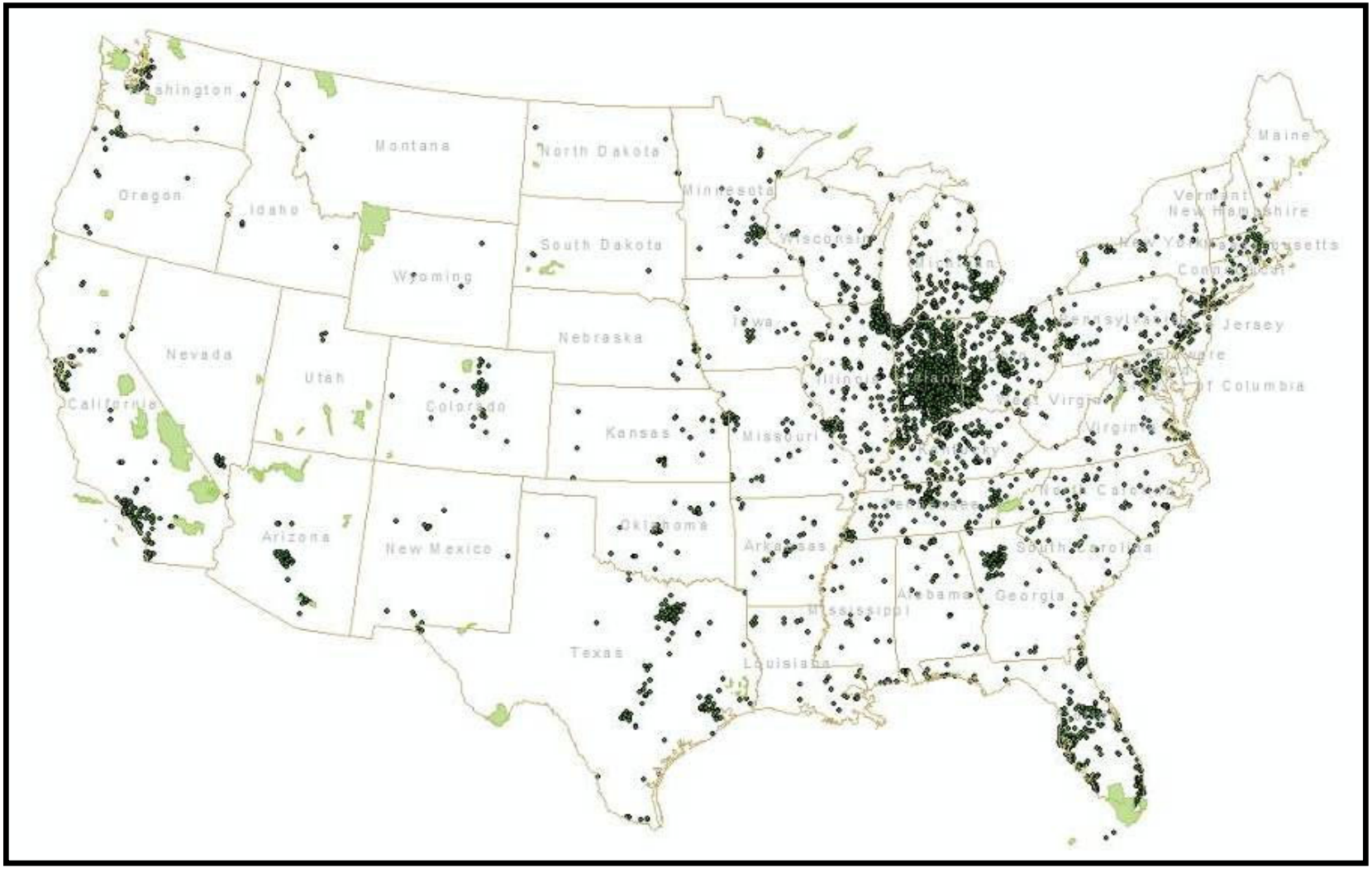

Fig. 1: Map prepared by Indiana Network for Patient Care, 2004. Dots represent home addresses of patients treated at an Indianapolis, IN hospital over a six-month period.